UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/918,326 | 07/30/2001 | Keith Alexander Harrison | 30006788-2 | 4475 |

7590 06/10/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

| EXAMINER | |
|---|---|
| SCHUBERT, KEVIN R | |
| **ART UNIT** | **PAPER NUMBER** |
| 2137 | |

DATE MAILED: 06/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/918,326 | HARRISON ET AL. | |
| | Examiner | Art Unit | |
| | Kevin Schubert | 2137 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *12 May 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *05122005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

Claims 1-16 have been considered. The examiner notes that the amendments to the specification and the claims have been considered, and the examiner believes no new matter has been entered.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 11 and 15-16 are rejected under 35 U.S.C. 102(e) as being anticipated by DeBry, U.S. Patent No. 6,385,728.

As per claim 11, the applicant describes a method comprising the following limitations which are met by DeBry:

a) using a unique identifier printed on the received document to search for a corresponding record in a list of received document records (Col 8, lines 6-36);

b) referencing a digital certificate associated with the selected record, the certificate being one of a store of certificates of received documents and each digital certificate being associated with a sender of the received digital document (Col 8, lines 6-36);

c) receiving an encrypted digest of the received digital document (Col 8, lines 6-36);

d) decrypting the encrypted digest (Col 8, lines 6-36);

e) computing a value of a second digest from the received digital document (Col 8, lines 6-36);

f) comparing the computed value of the second digest with a value of the decrypted digest (Col 8, lines 6-36);

g) carrying out an on-line authentication of the certificate when the computed value of the second digest corresponds with the value of the decrypted digest (Col 8, lines 32-36).

As per claim 15, the applicant describes a method according to claim 11, which is met by DeBry, with the following limitation which is also met by DeBry:

a) receiving a copy of a document (Col 8, lines 6-36);

b) computing a digest of the document copy (Col 8, lines 6-36);

c) comparing the computed digest with the decrypted digest (Col 8, lines 6-36);

d) determining that the document copy is authentic when the computed digest corresponds to the decrypted digest (Col 8, lines 6-36).

As per claim 16, the applicant describes a method according to claim 11, which is met by DeBry, with the following limitation which is also met by DeBry:

Wherein computing the digest of the document copy further comprises using a hash algorithm to compute the digest of the document copy, wherein the hash algorithm is the same as an original hash algorithm used to originally generate the decrypted digest (Col 8, lines 6-36).

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4,8-9, and 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over DeBry in view of Mandelbaum, EP Patent No. 0671830A2.

As per claims 1 and 10, the applicant describes a document printout device comprising the following limitations which are met by DeBry in view of Mandelbaum:

a) a store of digital certificates, each certificate being associated with a received digital document and a sender of the received digital document (DeBry: Col 8, lines 6-36);

b) an audit log comprising a list of received document entries, each entry containing a reference to one of the certificates in the store, an encrypted digest corresponding to the received digital document of that entry, and a unique identifier associated with the received digital documents (Mandelbaum: Col 7, lines 7-13; Table 404 of Fig 4; DeBry: Col 8, liens 6-36);

c) a decryption algorithm for decrypting the received encrypted digest associated with one of the received digital document selected for verification (DeBry: Col 8, lines 6-36);

d) a hash algorithm for creating a digest of the selected digital document such that when the created digest corresponds to the decrypted digest, the digital certificate of the sender is authenticated (Col 8, lines 6-36);

DeBry discloses all the above limitations except for the use of an audit log. Mandelbaum discloses a similar printing environment in which a print server maintains an audit log of received documents. Combining Mandelbaum into DeBry's system allows received will-call certificates to be stored in the print server in an audit log.

As per claim 2, the applicant describes a device according to claim 1, which is met by DeBry in view of Mandelbaum, with the following limitation which is met by DeBry:

Wherein the device is arranged to carry out an on-line authentication of a received certificate held in the store of received documents (DeBry: Col 9, lines 16-27; Col 8, lines 32-36);

As per claim 3, the applicant describes a device according to claim 2, which is met by DeBry in view of Mandelbaum, with the following limitation which is met by DeBry:

Wherein the device is arranged to carry out a batch of on-line authentications of received certificates held in the store of received documents (DeBry: Col 9, lines 16-27);

If more than one end-user sends the print server his certificate at the same time, authentication would take place in batch.

As per claim 4, the applicant describes the device of claim 1, which is met by DeBry in view of Mandelbaum, with the following limitation which is met by DeBry:

Wherein each entry in the audit log contains a digest of the received document to which it relates (DeBry: Col 5, lines 62-66; Col 6, lines 1-2);

As per claim 8, the applicant describes a device according to claim 1, which is met by DeBry in view of Mandelbaum, with the following limitation which is met by Mandelbaum:

Wherein each entry in the audit log contains the time and date of receipt of each digital document (Mandelbaum: Table 404 of Fig 4);

As per claim 9, the applicant describes the device of claim 1, which is met by DeBry in view of Mandelbaum, with the following limitation which is met by Mandelbaum:

Wherein the unique identifier is an alphanumeric code and the device further comprises an input module for inputting the code to access the relevant entry in the audit log (Mandelbaum: Col 7, lines 7-13);

As per claim 12, the applicant describes a device according to claim 1, which is met by DeBry in view of Mandelbaum, with the following limitation which is met by DeBry:

Wherein each digital certificate comprises a public key associated with a sender of the received digital document; wherein the decryption algorithm decrypts the encrypted digest using the sender's public key extracted from the digital certificate; wherein the hash algorithm computes a digest of a

document copy, and wherein the authenticity of the copied document is verified when the computed digest corresponds to the decrypted digest (Col 8, lines 6-36; Col 8, lines 59-61);

DeBry does not disclose that the will-call certificates contain a public key of the document source. This is probably due to the fact that the document source already has its public key so it doesn't need to put it on the will-call certificate for verification when it receives it back. However, DeBry does disclose that certificates commonly contain a sender's public key so the recipient can verify the sender. It would have been obvious to one of ordinary skill in the art to add the public key of the document source to the will-call certificate because doing so allows the print server to authenticate the document source.

As per claim 13, the applicant describes a device according to claim 12, which is met by DeBry in view of Mandelbaum, with the following limitation which is met by DeBry:

Further comprising a remote device that encrypts the digest of the received digital document using the sender's private key (Col 8, lines 6-36).

Claims 5-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mandelbaum in view of DeBry in further view of Fischer, European Patent No. 0386867B1.

As per claim 5, the applicant describes a device according to claim 4, which is met by Mandelbaum in view of DeBry (see above), with the following limitation which is met by Fischer:

Further comprising a hash algorithm for creating a digest of a digital document and a receiving module for receiving a digital representation of a previously printed out document, wherein the device is arranged to create a digest of the digital representation of the previously printed out document and to compare the newly created digest with the corresponding digest stored in the audit log (Fischer: Page 17, lines 21-36).

Mandelbaum in view of DeBry discloses all the limitations of claim 4. However, Mandelbaum in view of DeBry fails to disclose the use of printing out a document and then scanning it back in to create a new digest for comparison of a stored digest. Fischer describes a system where a document that is

printed out can be scanned back in. Upon doing this, a digest of it is created for comparison of it with a saved digital signature to make sure the document is genuine.

In the case where a user wants to verify that a printed out document is authentic or was printed out at a particular machine, a newly created digest could be used to reference an audit record via a saved digest. The newly created digest would be compared with saved digests, and if a match occurs, the corresponding audit record is pulled up which can verify whether the document was printed out at the particular machine and what time it was printed out for security or non-repudiation means. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Mandelbaum in view of DeBry, which disclose an audit log which maintains a digest of a document, with the ideas of Fischer, which disclose the use of creating a digest of a scanned in document, because the use of a digest to reference an audit record is an obvious alternative method to the use of referencing an audit record via an alphanumeric code as already described by Mandelbaum (Col 7, lines 7-13) and DeBry (Col 8, lines 27-31).

As per claim 6, the applicant describes a device according to claim 5, which is met by Mandelbaum in view of DeBry in further view of Fischer (see above), with the following limitation which is met by Fischer:

Wherein the device is arranged to send either a stored digest or a newly created digest of a document to its original sender to verify the authenticity of the document back to its source by considering the transmitted results of a comparison of digests carried out at the source (Page 18, lines 29-36);

Mandelbaum in view of DeBry in further view of Fischer disclose all the limitations of claim 5. Fischer also discloses a method whereby a document can be scanned in and a digest can be created for a document which can be transmitted and verified at a remote location of a recipient. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Mandelbaum and DeBry with those of Fischer and incorporate the idea of sending the computed digest to a recipient's location for authentication in the case that a recipient wants to authenticate a document.

As per claim 7, the applicant describes the device according to claim 5, which is met by Mandelbaum in view of DeBry in further view of Fischer (see above), with the following limitation which is met by all three references:

Wherein the receiving module is a document scanning module (Mandelbaum and DeBry: use of a fax machine (see claim 1); Fischer: Page 17, lines 28-36).

Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over DeBry.

As per claim 14, the applicant describes a method according to claim 11, which is met by DeBry, with the following limitation which is also met by DeBry:

Decrypting the encrypted digest using the public key of the sender extracted from the certificate (Col 8, lines 6-36; Col 8, lines 59-61);

DeBry does not disclose that the will-call certificates contain a public key of the document source. This is probably due to the fact that the document source already has its public key so it doesn't need to put it on the will-call certificate for verification when it receives it back. However, DeBry does disclose that certificates commonly contain a sender's public key so the recipient can verify the sender. It would have been obvious to one of ordinary skill in the art to add the public key of the document source to the will-call certificate because doing so allows the print server to authenticate the document source.

***Response to Arguments***

Applicant's arguments filed 5/12/05 with respect to claim 1 have been fully considered but they are not persuasive. The applicant argues that DeBry in view of Mandelbaum fails to disclose the authentication limitations present in the claim. The examiner disagrees. DeBry discloses maintaining a store of will-call certificates, at a document source, which contain the digital signature of the sender (the document source) (part a). The print server receives the will-call certificate (received document) which contain a reference to one of the certificates in the store on the document source, the digital signature of the sender, and a unique identifier associated with the document (part b). The use of maintaining

received documents in a log is disclosed by Mandelbaum. The print server also maintains a decryption algorithm for decrypting the digital signature of a received document (will-call certificate) (part c) and a hash algorithm for creating a digest of the selected digital document (part d). If the two digests match, the will-call certificate as originally sent is authenticated and a requested file is sent to the print server.

Applicant's arguments with respect to claim 11 have been fully considered but they are not persuasive. The applicant argues that DeBry is completely silent as to the method of authenticating as defined by the features of claim 11. The examiner disagrees. DeBry discloses a system in which a document source creates a will-call certificate in response to a user request to print a requested file. The document source copies the will-call certificate and sends one copy to the user and the other copy to its internal certificate store thereby maintaining a store of received documents (or certificates) with each certificate being associated with the sender of the received digital document because the certificate have the signature of the document source (part b). The user sends the copy of the will-call certificate to the print server which then sends a request to print back to the document source with the will-call certificate. The document source then uses the unique identifier printed on the received document (the received will-call certificate) to search for the corresponding will-call certificate stored in memory to make sure they are the same (part a).

Upon receiving the will-call certificate, the document source decrypts its digital signature and computes a second digest of the received document to authenticate the received document, or certificate (parts c,d,e, and f). Finally, if the computed value of the second digest is equal to the value of the decrypted digest, the document source carries out an on-line authentication of the certificate by sending the requested file to the print server (part g). If the computed values of the two digits are not the same, the document source would not carry out an on-line authentication of the certificate because it would not send the requested file to the print server.

***Conclusion***

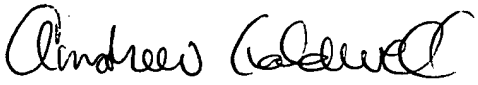
**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER